Pepco Holdings, Inc

701 Ninth Street, N.W.
Washington, DC 20068

William M. Gausman
Senior Vice President
Asset Management and Planning

202-872-3227
202-872-3302 Fax
wmgausman@pepco.com

July 12, 2010

U.S. Department of Energy
Office of the General Counsel
1000 Independence Avenue, SW
Room 6A245
Washington, DC 20585

Re: NBP RFI: Data Access

Pepco Holdings, Inc. (PHI) is pleased to respond to the U.S Department of Energy request for comments regarding the topics of data access, third party usage and privacy as they relate to consumers energy usage information and the Smart Grid.

PHI is one of the largest energy delivery companies in the Mid-Atlantic region. PHI's three electric distribution companies – Potomac Electric Power Company (Pepco), Delmarva Power (DPL), and Atlantic City Electric (ACE) – provide regulated electricity service to about 1.9 million customers in Delaware (DE), the District of Columbia (DC), Maryland (MD) and New Jersey (NJ).

To PHI, the question is not who "owns" energy consumption data, but how the data is protected and accessed. PHI believes customers have the right to privacy regarding energy consumption data, but that it must be recognized that utilities need to have an unconstrained right to access, control and use this information for legitimate utility-related purposes (e.g. network optimization, system planning, system operations, customer billing and credit and collection activities). The safe and secure operation of the Nation's power delivery network is the unique responsibility of the local distribution company (LDC) and the LDC must not be constrained in its ability to access and use customer energy consumption data for legitimate business and operational purposes.

Today, LDCs have access to customer usage information and are required to adhere to regulatory requirements concerning protection of such information. While implementation of Smart Grid will enhance the type and volume of information that can be accessed, reviewed and analyzed the existing regulations will continue to apply. The LDC should be the only "utility" entity that has access to this information without customer consent. Utility companies should continue to adhere to existing state and local regulatory and other legal requirements concerning protection of customer data and personal information. Each state that PHI operates within has adopted consumer protection statutes which provide for the protection of consumer data.

PHI believes that customer information should not be made available to third- party service providers without the full knowledge and consent of the customer. In addition, PHI believes that third- party service providers should be required to obtain state approval before they are deemed to be eligible to receive this information. Such third-parties should be subject to the same data privacy and security standards as the utility gathering the information.

National security requires that a high level of focus be placed on the security and protection of all aspects of the electric system and associated sub-systems. PHI believes that Smart Grid systems and components must be designed to against cyber and physical attacks. As the Smart Grid is implemented, applicable prudent security practices, policies and standards must be incorporated into these systems. It is PHI that has the obligation to serve our customers and it is PHI that has the ultimate responsibility to maintain the security of our customer's data as well as the security of the electric system. This responsibility is not taken lightly and being the electric utility serving Washington DC we can never accept any outside party directly accessing electric system data for the fear of reducing the level of security expected by our customers, regulators and national security organizations. Therefore it must be required that any third party have in place appropriate firewalls, encryption methods, etc., as may be established in accordance with the NIST Smart Grid Cyber Security Strategy and Requirements (NISTR 7628).

Today, as is common in the industry for utility networks currently being deployed, PHI is developing an AMI architecture that will allow for interval reads to be collected and provided to customers on a day-after basis. This architecture will also have the ability to securely provide raw usage and demand data directly to an In-Home Display that is registered within the customer's HAN. This information can include interval usage data, historical usage information, product details, critical event status and messaging. The ability to provide real time or near real time energy is applied to data associated with the operation of the electric system and typically is not available or needed for metering data. The cost to provide real time metering data to all customers would be cost prohibitive and outside of the capabilities of the systems being installed by most utilities today.

Background

PHI is implementing one of the nation's most advanced Smart Grid programs. PHI's Smart Grid program will enable customers to move towards energy reduction and improved energy management. It will also enhance grid reliability and optimize asset operations and maintenance. In addition, it lays the groundwork for wide-scale distributed renewable energy generation, electric vehicle adoption, carbon footprint reduction and increased energy security.

PHI's ongoing Smart Grid implementation has been accelerated due to the Smart Grid Investment Grant of $168.1M that PHI was recently awarded[1]. The program includes the implementation of Advanced Metering Infrastructure (AMI), Distribution Automation (DA), Demand Response (including Direct Load Control and Dynamic Pricing) and the enabling Communications Infrastructure (CI).

Specifically, PHI is currently:

- Installing over 1 .3 million smart meters equipped with network interface cards;
- Improving demand response capabilities by enabling dynamic pricing programs and installing approximately 300,000 AMI-enabled Direct Load Control (DLC) devices; and
- Deploying DA and CI technologies that will be leveraged by both AMI and DA

PHI's existing Smart Grid program not only delivers early benefits, but also provides the foundation for further expansion and enhancement. The implementation of the Smart Grid is an

[1]PHI's subsidiary companies, the Potomac Electric Power Company (Pepco) and Atlantic City Electric, received $44.6M for the Pepco (District of Columbia) Smart Grid Program, $104.8M for the Pepco (Maryland) Smart Grid Program and $18.7M for the Atlantic City Electric Smart Grid Program.

evolutionary process. The first step is for electric utilities to enhance grid visibility and control by installing intelligent devices (such as smart meters), expanding their communication networks and enhancing their monitoring and control systems. PHI believes that a nation-wide "one-size fits all" Smart Grid design is difficult to attain. Utilities service different electric distribution landscapes, are under different state regulation(s) and have assets capable of varying levels of existing automation – all of which present unique challenges.

As one of the electric utilities that has already moved forward with this first step, PHI understands that its technology choices need to consider the future evolution and interdependency of the nation's Smart Grid. It is important to note that these new smart grid capabilities must be enabled in an environment that respects the physical role of local transmission and distribution companies who, with Independent System Operators, oversee the safe and reliable delivery of energy while instantaneously balancing supply and demand among the stakeholders. PHI's design reflects these needs, using proven technologies to ensure that the Smart Grid is not only secure, but also interoperable and upgradeable in the future.

PHI recognizes the monumental task of understanding the consumer data access and privacy needs required for the Smart Grid, and would like to express their appreciation to the DOE for undertaking this effort. Thank you for the consideration of these comments.

To this end, PHI recognizes the criticality of staying at the forefront of not just Smart Grid technology developments in the marketplace, but the progression of Smart Grid-related regulatory, policy and standards as well. PHI welcomes DOE's interest in Smart Grid and appreciates this opportunity to respond to the attached questions.

Sincerely,

William M. Gausman

Pepco Holdings Inc

Questions and Answers

(1) Who owns energy consumption data?

To PHI, the question is not who "owns" energy consumption data, but how the customer specific data is protected and accessed. PHI believes customers have the right to privacy regarding customer specific energy consumption data, but that it must be recognized that utilities need to have an unconstrained right to access, control and use this information for legitimate utility-related purposes (e.g. network optimization, system planning, system operations, and customer billing, and credit and collection activities). The safe and secure operation of the Nation's power delivery network is the unique responsibility of the local distribution company (LDC) and the LDC must not be constrained in its ability to access and use customer energy consumption data for legitimate business and operational purposes.

(2) Who should be entitled to privacy protections relating to energy information?

As indicated above, PHI believes that customers have the right to privacy regarding customer specific energy consumption data. Such energy consumption data should not be made available to third party service providers, or others, without the full knowledge and consent of the customer. In addition, PHI believes that third-party service providers requesting such information should first be approved by the appropriate State regulatory authority to ensure that such entity is determined to be eligible to receive this information. The LDCs should not make this determination.

PHI supports granting customers the ability to authorize third-party access to their energy usage information so long as it is recognized that the utility will have the un-constrained right to access, control and use this information for legitimate utility-related purposes (e.g. network optimization, system planning, system operations, customer billing, etc.). The safe and secure operation of the overall power delivery network must be recognized and must remain paramount.

Further, utilities must retain the ability to recover all costs involved in obtaining, processing and using the information derived from its equipment, including meters.

(3) What, if any, privacy practices should be implemented in protecting energy information?

PHI believes that, while currently there are adequate measures in place within the jurisdictions in which it operates to protect energy usage information, additional measures will be needed as smart grid implementation expands.

Today, LDCs have access to customer usage information and are required to adhere to regulatory requirements concerning protection of such information. Further, LDCs have a strong track record of safeguarding the privacies and energy usage information of their customers based on

existing practices and regulatory structures. While implementation of Smart Grid will enhance the type and volume of information that can be accessed, reviewed and analyzed the existing regulations should continue to apply.

The LDC should be the only "utility" entity that has access to this information without customer consent. Utility companies should continue to adhere to existing state and local regulatory and other legal requirements concerning protection of customer data and personal information. Each state that PHI operates within has adopted consumer protection statutes which provide for the protection of consumer data. For example, in the District of Columbia, Title 34 of the District of Columbia Municipal Regulations sets forth those requirements. Section 34-1507 entitled, "Consumer Protections," provides:

> Unless a customer consents in writing, a market participant or the electric company may not disclose information that is about the customer; and was supplied to the marked participant or electric company by the customer. Unless a customer consents in writing, a market participant or the electric company may not use information of the type specified for any purpose other than the purpose for which the information was originally acquired.

This provision remains applicable to the enhanced data obtained through the Smart Grid. While several entities have raised concerns regarding privacy suggesting that states and localities have not adopted policies to protect customers from privacy breaches, PHI believes that. Smart grid does not require re-inventing the paradigm relative to consumer data protection. Existing regulations apply to the data that is generated by deployment of the Smart Grid.

(4) Should consumers be able to opt in/opt out of smart meter deployment or have control over what information is shared with utilities or third parties?

Unfortunately, it simply is not practicable for consumers to be afforded the opportunity to opt in/opt out of smart meter deployment. The deployment of "smart meters" is an integral component of the implementation of the Smart Grid. System design necessitates technological uniformity. The network's security and reliability features, comprehensive two-way communication system, administrative and operational efficiencies, and cost-benefit performance would be negatively impacted by piecemeal smart meter deployment.

The interests of the electric utility and the electric consumer are convergent and should be viewed in this manner as policies are developed and implemented to protect customer data and privacy and overall system reliability and security.

(5) What mechanisms should be made available to consumers to report concerns or problems with the smart meters?

As Smart Meter installations progress, the meters become merged into existing utility structures and processes. As such, consumers will be able to continue to contact the utility with questions

or concerns through existing communication channels (i.e, internet, Call Center, U.S. Mail). Consumers dissatisfied with the response they receive from normal communication channels may seek to escalate their complaint with the utility, or report concerns to the applicable Public Service Commissions (PSC) / Board of Public Utilities (BPU).

At PHI today, the Company's utilities receive customer concerns through a variety of methods. The most common mechanism consumer's use is direct inquiry through the Company's Call Centers. Customers who are dissatisfied with the manner in which their concern has been handled on line or through the Call Center can have their complaint escalated to a higher level manager or executive. Complaints received through a PSC / BPU, People's Counsel / Public Advocate or from an elected official are handled as 'escalated" complaints. Smart meter related concerns that are determined to require "escalated" handling will be processed in accordance with the escalated complaint process.

PHI's utilities also review and assess general customer inquiries and determine whether there is a common concern / issue which require comprehensive analysis and a holistic approach to formulating improvements. Smart Meter complaints will be handled in this matter to determine whether, based on the nature, frequency and type of complaints received, there is a process or procedure which should be analyzed and/or modified.

(6) How do policies and practices address the needs of different communities, especially low-income rate payers or consumers with low literacy or limited access to broadband technologies?

PHI believes that the same energy management capabilities should be available to all customers so that all will have the opportunity to participate in the programs and services offered. Utilities, unlike third-parties, have an existing obligation to serve all residential customers equally. The basic functionality laid out in PHI's Smart Grid architecture will provide the ability for low-cost, mass produced in-home devices, once developed, to interface with the HAN. Under the ZigBee Smart Energy Profile, these devices could interface with the meter directly to display energy usage information to the customer to provide the information necessary for the consumer to conserve and reduce or modify his/her energy usage. In addition, by capturing detailed interval data with the Smart Meter, utility companies can use this data to more effectively evaluate the benefits that various energy efficiency programs, such as home audits and weatherization, could specifically provide to low income customers.

PHI's utilities are very aware of the needs of the diverse communities they serve. To that end, policies are implemented to ensure balanced access to information, although the transmittal vehicle may differ. For example, Pepco had a very positive experience with low income participants when it implemented the Smart Meter Pilot Program, Inc. in the District of Columbia in partnership with the Consumer Utility Board, the District of Columbia Office of the People's Counsel, the District of Columbia Public Service Commission and the International Brotherhood of Electrical Workers. The program began in mid-July, 2008, and ended in October 2009. The participant population included residential customers of all income levels. The results of the study demonstrate that low income customers can and will respond to dynamic pricing rate signals, thereby lessening their electricity costs. There have been questions raised, nationally, concerning the responsiveness of lower-income communities to this new technology, which, ultimately,

requires behavioral changes. The Pilot showed that these communities can be reached. A variety of mechanisms are available to ensure that the low-income population, who may have low literacy and/or limited access to broadband technologies, still can avail themselves of these new opportunities and derive associated benefits. For example, access to the Internet is not required for critical peak event notification. PHI's utilities will use existing relationships with state social services agencies to reach the constituents they serve by providing them with outreach and general information.

Another way all customers benefit from Smart Grid investments is that they provide a means to manage current and future demands for electricity to ensure greater reliability and capacity of the grid. All consumers, including low income customers, will benefit from this network optimization.

(7) Which, if any, international, Federal, or State data-privacy standards are most relevant to Smart-Grid development, deployment, and implementation?

Data-privacy standards similar to those set for federal government agencies in FIPS-199 (Federal Information Privacy Standard), the Privacy by Design concept developed by the Information and Privacy Commissioner of Ontario, Canada, and those set for the financial services industry under the Gramm-Leach-Blilely Act should be considered for smart-grid development, deployment and implementation. Additionally, NIST is also evaluating new privacy exposures which may be created in Smart Grid environments, and identifying best practices for meeting these exposures.

Privacy by Design is a concept developed by the Information and Privacy Commissioner, Ontario, Canada. *Privacy by Design* refers to the philosophy and approach of embedding privacy into the design specifications of various technologies. This may be achieved by building the principles of Fair Information Practices (FIPs) into the design, operation and management of information processing technologies and systems. *Privacy by Design* extends to a "Trilogy" of encompassing applications:

1) Information Technology systems.
2) Accountable business practices.
3) Physical design and networked infrastructure.

The Information and Privacy Commissioner of Ontario Canada believes that *Privacy by Design* may be accomplished by practicing the 7 Foundational Principles, which have been specifically adapted to their Smart Grid context, to create Best Practices for Smart Grid *Privacy by Design*:

1. Smart Grid systems should feature privacy principles in their overall project governance framework and proactively embed privacy requirements into their designs, in order to prevent privacy-invasive events from occurring;
2. Smart Grid systems must ensure that privacy is the default — the "no action required" mode of protecting one's privacy — its presence is ensured;
3. Smart Grid systems must make privacy a core functionality in the design and architecture of Smart Grid systems and practices — an essential design feature;

4. Smart Grid systems must avoid any unnecessary trade-offs between privacy and legitimate objectives of Smart Grid projects;
5. Smart Grid systems must build in privacy end-to-end, throughout the entire life cycle of any personal information collected;
6. Smart Grid systems must be visible and transparent to consumers — engaging in accountable business practices — to ensure that new Smart Grid systems operate according to stated objectives;
7. Smart Grid systems must be designed with respect for consumer privacy, as a core foundational requirement.

FIPS-199 is the Federal Government's answer to data classification. Developed in response to the E-Government Act of 2002 (FISMA- Federal Information Security Management Act), it is a framework that can be easily understood, adopted and implemented. It is based upon two components: security objectives and potential impacts. The three security objectives addressed by FIPS-199 are:

- Confidentiality, defined as "preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information;"
- Integrity, defined as "guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity;" and,
- Availability, defined as "ensuring timely and reliable access to and use of information."

FIPS-199 has been widely adopted by the federal government, ties back to best practice guidance developed by NIST, and is consistent with the FISCAM (Federal Information System Controls Audit Manual) manual that is used in many federal security audits.

Gramm-Leach Blilely Act (GLBA) sets forth data-privacy provisions for financial institutions handling consumer data of equal or greater sensitivity to that likely to be collected by the Smart Grid. Under GLBA, major components were put into place to govern the collection, disclosure, and protection of consumers' nonpublic personal information with regard to privacy, safeguards and pre-texting protection.

- The privacy rules in GLBA require the regulated institutions to provide each consumer with a privacy notice at the time the consumer relationship is established and annually thereafter. The privacy notice must explain the information collected about the consumer, where (if at all) that information is shared, how that information is used, and how that information is protected. The GLBA-mandated notice must also identify the consumer's right to opt out of information being shared with unaffiliated parties. In the application of this standard to the Smart Grid, an 'opt in' approach to consumer choice regard information sharing with third parties may be more appropriate.

- The safeguard rule in GLBA requires that the regulated institutions develop a written information security plan that describes how the company is prepared for and plans to continue to protect clients' nonpublic personal information. The plan must include:
  - Denoting at least one employee to manage the safeguards;

- Constructing a thorough risk management plan for each department handling the nonpublic information
- Specifics regarding the development, monitoring and testing of a program to secure the information, and
- Specifics on how the safeguards would be changed as needed due to changes in how information is collected, stored and used.

The pre-texting rule in GLBA simply encourages regulated institutions to implement safeguards against social engineering. These safeguards include training employees to recognize social engineering attempts.

In addition, NIST is leading a significant effort as well. NISTIR 7628 efforts will devote a chapter to "Privacy and the Smart Grid". This will provide a framework for developing and documenting formal privacy policies.

(8) Which of the potentially relevant data privacy standards are best suited to provide a framework that will provide opportunities to experiment, rewards for successful innovators, and flexible protections that can accommodate widely varying reasonable consumer expectations?

Many states are developing and/or adopting additional measures for data privacy standards, as detailed in PHI's response number 7, above. While there does not appear to be a single existing standard that can be recommended, PHI believes that the utility industry is approaching this issue correctly. With the leadership of DOE and NIST guidance and recommendations for privacy standards can be proposed, commented on and implemented for the benefit of the industry and its consumers.

(9) Because access and privacy are complementary goods, consumers are likely to have widely varying preferences about how closely they want to control and monitor third-party access to their energy information: what mechanisms exist that would empower consumers to make a range of reasonable choices when balancing the potential benefits and detriments of both privacy and access?

PHI believes that customer information should not be made available to third- party service providers without the full knowledge and consent of the customer. In addition, PHI believes that third- party service providers should be required to obtain state approval before they are deemed to be eligible to receive this information. Such third-parties should be subject to the same data privacy and security standards as the utility gathering the information.
An 'opt in' system that requires customers to affirmatively ask that their information be shared with a third-party is the best way to both allow consumers to protect their privacy and yet have access to innovative energy –related services.

PHI further would suggest that customers be required to advise utilities if they want to change their 'opt-in' selection.

(10) What security architecture provisions should be built into Smart Grid technologies to protect consumer privacy?

National security requires that a high level of focus be placed on the security and protection of all aspects of the electric system and associated sub-systems. PHI believes that Smart Grid systems and components must be designed to against cyber and physical attacks. As the Smart Grid is implemented, applicable prudent security practices, policies and standards must be incorporated into these systems.

The planned Smart Grid systems should incorporate a layered security approach and include security measures such as authentication, authorization, encryption, detailed logging and auditing for the entire system, including the back-office systems and components, wide area network (WAN) and RF Local Area Network (RF-LAN) communication facilities, as well as at the level of the individual components.

Smart Grid solutions should apply guiding principles and policies for protection of these systems. These principles and policies should address both physical and cyber threats. Corporate policies should include the requirement to activate and implement all security features included within systems and components as recommended by the manufacturer, as well as implementation of industry best practices.

The first line of defense is encryption. Although encryption does not prevent intrusion it does make it nearly impossible for the intruder to use the data once it has been intercepted or otherwise obtained. Application layer encryption offers the highest level of protection and should be used whenever possible.

The use of firewalls, VLANs, encryption, and other methods as defined in technology standards to defend, deter, detect and minimize security threats should be employed in the Smart Grid systems. In order to assist with monitoring the many components of the Smart Grid, a centralized system should be established in order to control and isolate identified or suspected threats. All data should be isolated via VLANs or other methods. As data migrates through the different layers it should pass through a firewall. Firewalls provide a perimeter security control ensuring challenges between secured facilities and networks. Firewalls should be configured to pass only predefined services based upon application specific requirements. Any remote access to systems should require authentication before allowing any access to the system.

The use of 3rd party assessments on regular intervals will help identify vulnerabilities within the network. All identified vulnerabilities should be tracked and mitigation strategies developed to address the vulnerabilities.

Some of the key standards pertaining to cyber security are currently in draft form and scheduled to be finalized within the next year. Smart Grid system designers and component suppliers should closely follow the development of these standards. This ensures that the designer of these systems will have the knowledge to incorporate the latest industry standards.

(11) How can DOE best implement its mission and duties in the Smart Grid while respecting the jurisdiction and expertise of other Federal entities, states and localities?

DOE has had tremendous success promoting the modernization of the grid through the strategic application of its grant funds and low cost loans. Recognizing not only the potential value of greater uniformity in standards in the area of data privacy but also the fact that jurisdiction over customer-utility interactions rests with the states, a model standard approach may be the most effective way for DOE to implement its mission and duties with regard to data privacy and the Smart Grid while respecting the jurisdiction and expertise of the states. PHI also believes that DOE may wish to consider an active role in educating consumers about the Smart Grid's capabilities and its advantages for consumers.

Specifically, an inclusive, collaborative approach may result in state adoption of the model standards where permitted by or consistent with state law. PHI believes it likely that DOE could maximize the potential for state adoption of model standards if it were to establish a working group, comprised of representatives from the policy divisions of the interest groups representing the key interests of state and local governments and regulatory bodies (National Council of State Legislatures, National Association of Counties, National League of Cities, National Association of Regulatory Utility Commissioners, National Association of State Utility Consumer Advocates), with specialized expertise in this area. It is also critical that representatives of the utilities have a defined role as this piece is developed.

With regard to other Federal entities, DOE should coordinate its efforts in the data privacy arena with the efforts of other Federal agencies including the FCC, NIST and FERC. In particular, NIST has done considerable work in developing data privacy standards for application to federal agencies that may be tailored to fit the Smart Grid arena. PHI has devoted significant resources in assisting NIST in its efforts.

(12) When, and through what mechanisms, should authorized agents of Federal, State, or local governments gain access to energy consumption data?

PHI believes that State Public Service Commissions and energy agencies are likely to have need for access to aggregated energy consumption data for regulatory and energy planning purposes. PHI is also supportive of Federal agencies having access to aggregated energy consumption data for national energy planning purposes. PHI can support aggregated data sharing with those governments particularly under defined data sharing protocols that are web or other data platform-based, that require minimal administrative time and effort, and that protect individual customer data from disclosure. PHI believes that individual customer data cannot be released, even to governmental entities, without the customer's prior authorization, or subpoena or other court order.

.

(13)What third parties, if any, should have access to energy information? How should interested third-parties be able to gain access to energy consumption data, and what standards, guidelines, or practices might best assist third parties in handling and protecting this data?

Only those third parties that are registered by the state or local jurisdictions, such as third party energy providers, who have permission from the customer, should have access to a specific customer's energy consumption data. These third parties must be legally, morally and ethically bound to maintain the confidentiality of the customer's personally identifiable information (PII) in order to be registered and must to agree not to correlate data obtained from PHI with other sources or the individual, without consent of the individual. Methods such as pseudonymization or anonymyzation of identity will be used to ensure that customer personal identifiable information can be separated from customer energy consumption data where possible.

It should be remembered that Smart Meters are installed by the utility for the purposes of revenue metering and to provide the customer with electrical usage information to facilitate reducing their overall energy consumption. Eventually, customer energy consumption data will be sent directly from the AMI Meter to an in-home display or the customer's home energy management system through a one-way communication medium such as Zigbee, Home Plug, etc. (as long as it is compatible with the utility's AMI meter). Only registered third parties should be permitted access to this information. The State registration process should require that such third-parties have in place appropriate firewalls, encryption methods, etc., as may be established in accordance with the NIST Smart Grid Cyber Security Strategy and Requirements (NISTR 7628).

(14) What forms of energy information should consumers or third parties have access to?

Provided that data requests are processed in accordance with existing rules and regulations, consumers should have access to their usage (kWh) and demand (kW, if applicable) data as well as billing data. They should also have access to their own interval usage data. Consumers may authorize the utility to disclose the above referenced data to third parties. As stated above data should not be shared with third parties without customer consent.

(15) What types of personal energy information should consumers have access to in real-time, or near real-time?

PHI is concerned that the real-time information to customers for the customer specific energy usage data argument does not include discussions on the cost-benefit analysis. PHI believes that the real-time capabilities, as proposed by many in the industry, will require extensive incremental communication infrastructure as well as IT computing and storage capabilities and will provide limited customer benefits.

PHI' current proposal for AMI data collection include collecting data at 60-minute interval data for most customers and 15-minute interval for large commercial and industrial customers. As is common in the industry for utility networks currently being deployed, the interval data will be validated, estimated, edited against customer bill and then presented on its web site daily, on a

"day after use" basis. PHI has documented business case analysis, demonstrating customer benefits.

One of the likely real to near real-time option could include a presentation of the data closer to its time of actual usage, perhaps available more frequently than daily. PHI's smart meters contain a network interface card that houses a transmitter that uses the Zigbee protocol for short range radio transmissions. This Zigbee enabled capability could be used to transmit raw electricity usage data from the meter multiple times a day into the customer's home to one of a variety of devices. These devices include in home displays, programmable controllable thermostats that have a display or a wireless router used in a personal computer local area network. The infrastructure needed to meet the real-time access will depend largely on the type of data to be provided to the customer. For instance, instantaneous KW, KWh and total KWh can be obtained directly from the meter to an in-home display using the existing clusters within the Smart Energy Profile. Cost related information will require interfacing more back office systems and will probably be available over longer intervals. This alternative will provide near-real time validated data to the customer but not without significant incremental costs.

The other option being pursued by several thought leaders is to provide auditable (billing quality data) real-time or near-real time data to customers, which is also communicated and stored at utility offices for billing and audit purposes. The incremental costs for this alternative, for the utility, would be to design and test the interoperability of technologies and then educate customers regarding this capability. PHI also anticipates significant incremental costs for us to retrieve the real time or near real time data back in to our billing systems – which include significantly more additional capacity for the communication infrastructure, IT storage and computing resources and manpower. PHI has not conducted a cost benefit analysis on this topic, but anticipates that this would be a very costly undertaking.

It is also unclear at this time how in-home display devices will be rolled out to customers and who would pay for them.

(16) What steps have the states taken to implement Smart Grid privacy, data collection, and third party use of information policies?

Based on research and outreach to entities that represent state and local entities on the national level (NCSL and National League of Cities), to date, states and cities have not taken formal steps (legislation, ordinances, etc.) to specifically address Smart Grid privacy and data collection, with the exception of California and Texas. However, states and localities adhere to established consumer protections that involve protecting customer information from unauthorized third parties, including established notification protections should that information be breached or compromised. Under existing laws in the states in which PHI operates, the utility is required to notify customers if there is a breach of its security systems under certain circumstances. The utility is also required to protect customer data and adhere to specific laws and regulations concerning the release of that information. There has been new discussion, since ARRA, concerning developing and adopting measures that are specific to AMI-related data. Existing statutes:

Breach Notification

- For example, under 6 Delaware Code § 12B-101, et seq., a commercial entity that conducts business in Delaware… shall, when it becomes aware of a breach of the security of the [electronic data] system, conduct in good faith a reasonable and prompt investigation to determine the likelihood that personal information has been or will be misused. If the investigation determined that the misuse of information about a Delaware resident has occurred or is likely to occur… the commercial entity shall give notice as soon as possible to the affected Delaware resident."

- Under the Maryland Personal Information Protection Act, codified at MD Code Comm. Law § 14-3501, et seq., a company has an obligation to notify individuals as soon as reasonably practicable after notification or discovery of a breach of a system containing personal information. Pursuant to the statute, notification is required if after investigation, the business concludes that misuse of the individual's personal information has occurred or is reasonably likely to occur as a result of the breach.

- New Jersey (NJSA 56:8-161, et. Seq.) Provides for the notification of a data breach to individuals in the most expedient time possible and without unreasonable delay. The statute requires that the company report the breach to the state police before disclosing the breach to individuals.

- In the District of Columbia, consumer privacy relative to breach notification is protected under the Consumer Security Breach Notification Act, codified at D.C. Code § 28-3851, et seq. Under this Act, "[any]… entity who conducts business in the District of Columbia… who discovers a breach of the security of the electronic data system, shall promptly notify any District of Columbia resident whose personal information was included in the breach. This notification must be made at the earliest time possible and without reasonable delay. This statutory notification requirement is triggered if the breach includes a consumer's "personal information," as defined by the statute.

Release of Customer Information

.

- The District of Columbia Public Service Commission issued a notice of proposed rulemaking in Formal Case No. 1009 that, if adopted would continue the prohibition on providing customer-specific information with third parties unless the customer directs otherwise in writing (57 D.C. Register 989 (January 22, 2010) ("Title 39: Affiliate Transactions Code of Conduct"). Section 3903.1 of that notice provides: "An energy utility shall not disclose any customer-specific information obtained in connection with the provision of regulated utility services except upon written consent of the utility customer. The consent form signed by the utility customer shall state the purpose of the disclosure.

  Additionally, in the District of Columbia, disclosure of customer specific data is addressed by both the current code of conduct as well as the new Affiliate Transactions

Code of Conduct regulations that the Commission has proposed. To transmit information without the customer's consent would also likely violate Section 34-1507 of the District of Columbia Official Code, referenced earlier. Unless a customer consents in writing, a market participant or the electric company may not disclose information that is about the customer and was supplied to the market participant or electric company by the customer. This restriction does not apply to lawful disclosures for bill collection or credit rating reporting purposes. Unless a customer consents in writing, a market participant or the electric company may not use information for any purpose other than the purpose for which the information was originally acquired.

- In Maryland, pursuant to Public Utility Companies Article § 7-505(b0(6), electric companies and electricity suppliers shall not disclose a retail electric customer's billing, payment, and credit information without the retail electric customer's consent, except as allowed by the Commission for bill collection or credit rating reporting purposes. Pursuant to MD Code Comm. Law § 14-3503, to protect personal information from unauthorized access, use, modification, or disclosure, a business that owns or licenses personal information of an individual residing in the State shall implement and maintain reasonable security procedures and practices that are appropriate to the nature of the personal information owned or licensed and the nature and size of the business and its operations. A business that uses a nonaffiliated third party as a service provider to perform services for the business and discloses personal information about an individual residing in the State under a written contract with the third party shall require by contract that the third party implement and maintain reasonable security procedures and practices that are appropriate to the nature of the personal information disclosed to the nonaffiliated third party; and are reasonably designed to help protect the personal information from unauthorized access, use, modification, disclosure, or destruction.

  COMAR 20.40.02.01 (B)(5) – A utility may not except with the informed consent of the customer and in compliance with the Commission's consumer protection regulations, disclose any customer-specific information obtained in connection with the provision of regulated utility service. Pursuant to Maryland regulations, a supplier may not disclose a customer's billing, payment, and credit information without the customer's consent. However, s supplier may disclose a customer's billing, payment, and credit information for the sole purpose of facilitating billing, bill collection, and credit reporting. The supplier is required to provide a customer with a copy of the supplier's customer information privacy policy (COMAR 20.53.07.02).

- In New Jersey, an electric public utility, and a gas public utility shall not disclose, sell or transfer individual proprietary information, including, but not limited to, a customer's name, address, telephone number, energy usage and electric power payment history, to a third party without the consent of the customer (NJSA § 48:3-85). An electric public utility or a gas public utility may disclose and provide, in an electronic format, without the consent of a residential customer, a residential customer's name, rate class, and account number, to a government aggregator that is a municipality or a county, or to an energy agent acting as a consultant to a government aggregator that is a municipality or a county, if the customer information is to be used to establish a government energy

aggregation program, pursuant to explicit sections of the law. Whenever any individual proprietary information is disclosed, sold or transferred, pursuant to this section, it shall be used only for the provision of continued electric generation service, electric related service, gas supply service or gas related service to that customer. In the case of a transfer or sale of a business, customer consent shall not be required for the transfer of customer proprietary information to the subsequent owner of the business for maintaining the continuation of such services.

- In Delaware, pursuant to 26 Del. Admin. Code 3001-3.7, an electric supplier may request a list from an Electric Distribution Company which contains Retail Electric Customer's name, service address and mailing address. A Retail Electric Customer may elect to opt out of the list. Pursuant to 26 Del. Admin. Code 3001-5.5, an Electric Supplier, including Brokers, shall not engage in fraudulent or improper activities, nor shall it disseminate any consumer information obtained pursuant to Section 3.7, and may be subject to penalties as described in the Rules.

Smart Grid Data Protection

On February 19, 2010, Senate Bill 1476 was introduced in the California legislature. The proposed measure would add new sections to the Public Utilities Code. Under existing law, the Commission is required to conduct a pilot study of certain customers of each electrical corporation to determine the relative value to ratepayers of information, rate design, and metering innovations using specified approaches, but prohibits this data from being used for any commercial purpose, unless authorized by the customer. This bill would repeal the provisions relating to the study, and would require an electrical corporation or gas corporation that utilizes an advanced metering infrastructure that allows a customer to access the customer's electrical or gas consumption data, as defined, to ensure that the customer has an option to access that data without being required to agree to the sharing of his or her personally identifiable information, including electrical or gas consumption data, with a 3rd party. The bill would prohibit an electrical corporation or gas corporation from sharing, disclosing, or otherwise making accessible to any 3rd-party a customer's electrical or gas consumption data, except as specified, and would require those utilities to use reasonable security procedures and practices to protect a customer's electrical and gas consumption data from unauthorized access, destruction, use, modification, or disclosure. This bill would prohibit an electrical corporation or gas corporation from selling a customer's electrical or gas consumption data or any other personally identifiable information for any purpose (Amended, June 10, 2010).

Colorado

CO S 180, the "Smart Grid Task Force" was introduced on March 3, 2010 and enacted on June 11, 2010. The legislation requires the convening of a task force to recommend legislative and administrative measures to encourage the orderly implementation of smart grid technology in Colorado. The Task Force is required to develop an initial report, designated the 2011 Colorado Smart Grid Report, in which the Task Force addresses and makes recommendations for the following:

(I) Issues related to the utility side of the meter in the development of a Smart Grid, including: (A) Grid Reliability; (B) Grid Efficiency; (C) Outage Restoration and Recovery; (D) Distributed Generation Integration; (E) Transportation Electrification; and (F) System integration of renewable and conventional sources of electric power generation.

(II) Issues related to the customer side of the meter in the development of a Smart Grid, including: (A) Consumer Metering Protocols; (B) Driving Increases in Consumer Efficiency; (C) Providing Effective Consumer Information; (D) Integration of Demand Response Programs; and (E) Integration of Variable Pricing Mechanisms.

(III) Potential Impact from the Development of a Smart Grid, including: (A) Consumer Protection and Privacy; (B) Cyber Security; (C) Communication and Technical Standards; (D) Workforce and Economic Development Issues; (E) Energy Efficiency and Demand Response; and (F) Emissions from Electric Generation.

The initial report is due on or before June 20, 2011. The Task Force is required to meet at least annually, thereafter, to review the report, receive, and add information and to consider updates to the report.

Maine (Public Law No. 539)

This law establishes a state policy on smart grid infrastructure including employment of a smart grid to improve power reliability as well as the overall efficiency of the power resource and delivery system while reducing energy consumption, greenhouse gas emissions and costs to consumers, in part by offering consumers greater choice and information about their electricity consumption. The state policy ensures that deployment of a smart grid is done in a manner that is consistent with applicable safety, security and reliability standards. The bill includes legislative findings regarding the high cost of electricity to consumers, the need for smart grid electric infrastructure, the lack of a state policy on smart grid infrastructure and the need for such a policy.

This law allows transmission and distribution utilities to recover reasonable costs associated with creating a smart grid. It also directs the Public Utilities Commission to examine the need for and feasibility of creating or designating a special entity in each transmission and distribution utility service territory to facilitate a rapid increase in the availability and use of smart grid functions.

The Texas Public Utility Commission has issued the following rule (section 25.130(j)) governing meter data sharing:

(j) Access to meter data.

(1) An electric utility shall provide a customer, the customer's REP, and other entities authorized by the customer read-only access to the customer's advanced meter data, including meter data used to calculate charges for service, historical load data, and any other proprietary customer information. The access shall be convenient and secure, and the data shall be made available no later than the day after it was created.

(2) The requirement to provide access to the data begins when the electric utility has installed 2,000 advanced meters for residential and non-residential customers. If an electric utility has already installed 2,000 advanced meters by the effective date of this section, the electric utility shall provide access to the data in the timeframe approved by the commission in either the Deployment Plan or request for surcharge proceeding. If only a Notice of Deployment has been filed, access PROJECT NO. 31418 ORDER PAGE 94 OF 109 to the data shall begin no later than six months from the filing of the Notice of Deployment with the commission.
(3) An electric utility shall use industry standards and methods for providing secure customer and REP access to the meter data. The electric utility shall have an independent security audit of the mechanism for customer and REP access to meter data conducted within one year of initiating such access and promptly report the results to the commission.
(4) The independent organization, regional transmission organization, or regional reliability entity shall have access to information that is required for wholesale settlement, load profiling, load research, and reliability purposes.
(5) A customer may authorize its data to be available to an entity other than its REP.

(17) What steps have investor owned utilities, municipalities, public power entities, and electric cooperatives taken to implement Smart Grid privacy, data collection and third party use of information policies?

On an on-going basis, PHI reviews and enhances its policies and procedures regarding the protection of the confidentiality of PII within the control of the company, whether residing within the company or under the custody of a third party vendor. The policy includes, but is not limited to, Smart Grid data. Individuals covered by this policy include employees, contractors, customers, and shareholders.

Access to personal information is limited to those who require access by reason of their job duties. Information is provided to ensure that affected personnel are informed of the requirements for safeguarding personal information. Information identified as personal information is subject to controls to maintain its confidentiality. All personnel who have access to personal information are and will be required to follow the procedures established to protect this information.

Access to customer data by third parties will only be allowed with the explicit consent of the customer. Third party agreements will include restrictions on further sharing of the information, requirements for notification to each party in the case of a breach, required security controls, and other relevant factors. Also, Interconnection Security Agreements (ISA) will be used for technical requirements, as necessary. These agreements ensure that the third party organizations abide by rules for handling, disclosing, sharing, transmitting, retaining, and using the organization's personal information.

(18) Should DOE consider consumer data accessibility policies when evaluating future Smart Grid grant applications?

Yes, DOE should consider consumer data accessibility when evaluating future Smart Grid grant applications.

DOE has shown significant leadership in advancing the smart grid technologies and programs in the Nation by initiating the Smart Grid Investment Grants and Smart Grid Demonstration projects, which has immensely helped US utilities and manufacturers. These DOE programs have accelerated Smart Grid technology R&D and deployment efforts – which will act as a catalyst for significant investment and Smart Grid advancement in the next few years. This has put DOE in a leadership position to navigate the future of the Smart Grid particularly concerning consumer data accessibility and privacy. If DOE makes this an important criteria for future grants and provides guidance and template for consumer data accessibility, this will significant advance the issues around consumer information privacy.